International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Forensic Tools for Windows Forensic Analysis: A Comprehensive Review

Khaled Redwan, Jesmin Akhter and Abu Sayed Md. Mostafizur Rahaman

Jahangirnagar University, Savar, Dhaka, 1342, Bangladesh
khaled.rafsan1995@gmail.com; jesmin@juniv.edu; asmmr@juniv.edu

ABSTRACT

Windows forensic analysis is critical in digital investigations because it allows investigators to find significant evidence within Windows operating systems. Traditional forensic procedures are having difficulty keeping up with the shifting environment of digital crime due to the rising complexity of new cyber threats. In order to overcome these issues, academics and practitioners have turned to machine learning, a powerful branch of artificial intelligence, to improve the efficacy and efficiency of Windows forensic investigation. Because of their capacity to learn from data, find patterns, and make predictions or classifications, machine learning techniques have gained popularity in a variety of disciplines. A significant number of research papers have been investigated based on the ML approach to perform forensic investigation using Windows file history, jump list, prefetch file, and private browsing. It allows for the creation of complex models capable of detecting and classifying malware, spotting abnormalities in system behavior, evaluating event logs, and reconstructing event timelines.

Keywords: Windows forensics, Machine Learning Forensic tools, OS investigation procedure, Tools for Windows forensic

1. Introduction

Windows forensic is now a crucial investigation in Digital forensic world. With the combination of machine learning at Windows forensic analysis provides various benefits. It allows for the creation of complex models capable of detecting and classifying malware, spotting abnormalities in system behavior, evaluating event logs, and reconstructing event timelines. Investigators can handle and analyze massive amounts of data more efficiently by employing machine learning techniques, allowing for faster detection of suspicious actions and pertinent evidence. In this paper, we will review the current landscape of Windows forensic analysis and delve into machine learning applications and forensic tools in this context. We have discussed on five windows artifacts which is very crucial in case of windows forensics, we have also reviewed which forensic tools and Machine learning applications can help on the forensics of these artifacts.

2. Literature Review

While Windows operating systems (OS) are extensively used across the world, they are a major target for hackers. Traditional forensic techniques may not be sufficient to detect and evaluate Windows OS-related occurrences because of the cyber assaults. Machine learning (ML) has emerged as a viable way to improve Windows OS forensic investigations by providing automated and intelligent methods for discovering, classifying, and evaluating digital evidence. This literature review basically helps us to investigate the latest actions and problems in the field of Windows OS forensics utilizing machine learning techniques.

To discover relevant research publications published between 2015 and 2023, a systematic search was undertaken utilizing recognized sources; such as IEEE, ACM DL, and Google Scholar. The search terms included combinations of "Windows OS," "forensics," "machine learning," "malware detection," "behavior analysis," and "digital evidence."

We have reviewed the whole literature in such a sequence, where one can understand, what is digital Forensic and the role of machine learning in the field of digital forensic [1] [2] [3]. We have also discussed on the work flow model of digital forensic [4]. Secondly, we focused on windows forensic. We have discussed about windows [5] and its importance as it is a major target for cyber-attack [1]. Regarding contribution of ML in windows forensic we have clearly discussed on how the cyber-attack can be detected by Machine learning in case of windows forensic [6] [7]. As we know forensic tools plays a vital role in the field of digital forensic. Here we have discussed on the list of forensic tools for windows forensic and forensic of the windows artifacts [1] [8]. Lastly, we have discussed what windows artifacts are [9], and discussed 04 major windows artifacts forensic such as: windows File history [10] [11], Event Log [12][13] [14][15] ,Prefetch File [16].& Private browsing[17].

3. Windows forensic and Contribution of ML regarding Investigation

(3.1) Digital Forensic and the role of Machine Learning

Digital Forensics is a computer forensic investigation and analysis that includes capturing, preserving, analyzing, and presenting computer-related evidence [1].

At [2] a Digital investigation procedure is discussed. As like as the smart grid environment, for Windows forensic, we can also maintain these investigation procedures. Figure 1 shows major phases in digital forensics:

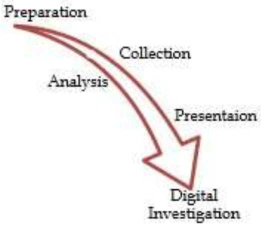

Figure 1: Investigation Procedure

For understating proper investigation practices, we have to maintain the workflow model of digital forensics. The investigation process is divided into some stages [4]

1. Data Seizure and Planning for Pre-devices
2. Identification-Handling-Preservation & Collecting
3. Post-Device or Data Seizure & Planning
4. Exhibit Handling
5. Data acquisition
6. Data Processing
7. Analysis, Interpretation, and Evaluation
8. Result Showcase
9. Review and
10. Completion of the Case

Various applications make use of machine learning algorithms and methods. For developers and forensic investigators in the field of machine learning, possessing a comprehensive grasp of the utilized algorithms, their functioning, and their ability to learn from raw data is essential for enhanced efficiency. The article [3] describes some Machine Learning algorithms such as: Support Vector Machine, Decision Tree, Naïve Bayes Classifications, K-nearest neighbors & artificial neural network for Link analysis, Clustering incidents and crimes, Predicting attacks and crimes and fraud detection.

(3.2) Windows Forensic

Operating system is the software which power up every-trends device we use. Windows is the most user-friendly OS for its graphical interfaces [5] . In the computer business, Windows is the most widely used OS. According to earlier forensic research, Windows is a major target in cybercrime as we know, the operating system is the key component for accessing hardware. A cybercriminal can meddle with the operating system in order to tamper with the evidence. Forensic specialists also discover that Windows is the first digital element that can reveal information about a data breach [1]. Most of the time Operating system faces the malware attack. At [5] we can see a survey which provide us the types of cyber-attacks on OS. Figure 2 will describe the scenario of the attacks.

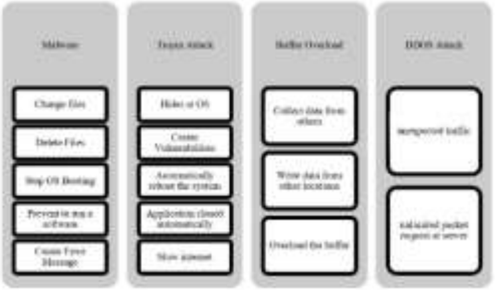

Figure 2:Cyber-Attack on OS

(3.3) Contribution of ML in Windows Forensic:

The article [6] indicates malware detection procedure through ML and Deep Learning. Where we will get a great ML technique to detect malware on all kind of artifacts but our main concern is about Windows forensic. The article examines the threats and weaknesses in Windows operating system security. It emphasizes that thieves are particularly targeting Windows 10, with a large number of security breaches detected. In addition, the paper discusses the frequency of security flaws in Windows Server 2016 and 2019. According to the author, Windows trojans account for a sizable portion of malware, and other sorts of assaults such as ransomware attacks or bot attacks and Trojans that attacks on Password, are also on the increase. The article describes many approaches for detecting Windows malware. These solutions require the use of machine learning (ML) techniques, such as developing an active learning malware detection framework and deploying Support Vector Machine classifiers etc. Here they used:

(1) Ratscope = Event Tracking for Windows

(2) SVM, Naïve Bayes = Sandboxing, Active Learning

(3) SVM Wrapper = Behavior of a runtime Environment

The article [7] discusses on ransomware detection using the Random Forest, Naïve Bayes, J48, Decision Table and Hoeffding tree. Table 1 discusses the accuracy of these ML Classifier for Malware Detection.

Table 1: Accuracy of ML Classifier for detecting Malware

SL	ML Classifier	Accuracy
1	Random Forest	0.997
2	Naïve Bayes	0.993
3	J48	0.997
4	Decision Table	0.987
5	Hoeffding tree	0.992

(3.4) Contribution of forensic tools for Windows Forensic:

Forensic tools play a vital role in digital forensic. Some of the forensic tools are discussed at [1] for windows forensic. such as,

(1) Access Data

(2) Pro discover Basic

(3) Autopsy

Table 2: Features of forensic tools

SL	Tool	Paid or Open Source	Features
01	Access Data	Paid	Create forensic images from various storage
			Password recovery solutions

			Process the data accurately
			Support different file system
02	Pro-discover Basic	Paid	Extract Data
			Extract deleted files
			Create Report
03	Autopsy	Open Source	Collect data
			Analyze data
			Recover photos from camera

At [8] provides us a basic information on some forensic tools for windows artifacts

Table 3: Uses of Forensic tools as per Windows Artifacts

Artifacts	Tools							
	Autopsy	Redline	Belkasoft	OS-Forensic	Prodiscover	x-ways	Encase	FTK
Windows File history	✓	✓	✓	✓	✓	✓	✓	✓
Event Log	✓	✓	✓	✓	✓	✓	✓	✓
Prefetch	✓	✓	✓	✓	✓	✓	X	✓
Private Browsing	✓	X	✓	✓	X	X	X	✓

4. ML & Forensic tools for Windows Artifacts Forensic

Artifacts refer to elements or regions within a computer system that store significant information pertaining to the user's actions on the computer. The nature and location of information found in these artifacts can vary across different operating systems. Identifying these artifacts, processing them correctly, and analyzing the information they contain are essential steps in substantiating or refuting observations made during forensic analysis. It's crucial to note that the absence of information in a specific artifact does not necessarily negate the occurrence of an activity within the computer system. In the Windows environment, numerous artifacts function as crucial evidence in the forensic examination of digital media. Moreover, the types and locations of these artifacts may exhibit variations among distinct versions of the Windows operating system.[9]

Here we have selected five artifacts at the time of Windows forensic:

(1) Windows File History

(2) Event Log

(3) Prefetch File

(4) Private Browsing

We have also reviewed the solution/tools as per these artifacts in case of forensics.

(4.1) Windows File History

File History (FH), a feature introduced since Windows 8, is a user-configurable backup function. It can be activated with various storage devices and functions according to user-defined settings, such as 'backup cycle' and 'backup target folders.' Once enabled, FH initiates the backup process for files within the specified backup target folders. To optimize storage usage, FH monitors changes in Update Sequence Numbers (USN) for backed-up files, selectively performing backup operations only for modified or newly added files.

Since Windows 8, File History (FH) serves as a user-controlled backup functionality. Users can configure and activate FH by choosing a storage device for backing up files, which may include local drives, USB flash drives, network drives, and more. This unique backup feature facilitates file restoration and the removal of older backup versions as needed. Consequently, the analysis of forensic artifacts indicating user actions regarding FH becomes crucial when examining Windows systems.

Machine Learning for File History Forensic:

We can use Feed Forward Neural Network, Support Vector Machine, Random Forest, Classifications and Regression Trees as these algorithms were chosen due to their diverse approaches in generating classifiers and their frequent use in constructing classification models. Furthermore, the selection of these algorithms aims to evaluate the effectiveness of various learning strategies within the realm of file history forensics. [10]

Tools for File History forensic: The authors created an open-source solution named “EFIC”,[11] the tool that can analyze FH and Users may utilize the tool for the extraction and normalization of the FH related data like as files back up, files restore, associated the registry entries.

(4.2) "Event Log”

As per Microsoft TechNet, the event log is a service that logs event message occurred by programs and Operating system. A forensic investigator can get a clear detail about applications, user login timestamps and system events through the event log. [12]. Event logs are recordings of computer system events and activities that provide useful information for troubleshooting, security analysis, and system monitoring. Windows keeps many events log files, such as

System logs: System logs captured by windows system component. example: At the time of startup, the failure of a driver

Security log: Security log captures security events. Example: valid invalid logon details.

Log of applications: Application logs capture events by programs. Example: A database program can record a file error. [13] [12] .

Machine Learning for event log forensic: Nerlogparser [14] is developed in python 03, it uses TensorFlow for deep learning library

Tools for event log forensic: Event Viewer [15] is one of the apps of Windows 10 &Windows 11. This log viewer collects events log of applications, setup, system and many more events that are created on a PC. The interface is very user-friendly for solving error and difficulties.

Park S, Lee S [13] developed a solution named DiagAnalyzer which can gather the below information mentioned in Table 4 from the user.

Table 3: Information gathered by DiagAnalyzer

SL	Category	Information
1	General	Name and Version of the OS, Device Manufacture, Name of the device model
2	USB	Serial number, manufacture, fire system
3	Web	Browser Application, version, web page visited, title of the web pages.
4	Wireless	Access point Status (Hidden), Cipher Algorithm, Authentication algorithm,

The Link of DiagAnalyzer is: https://github.com/francOSax/DiagAnalyzer

(4.3) Prefetch File

The Prefetch file is a component in Windows operating systems that helps simplify the startup process and enhance the performance of frequently used apps. Prefetch analyzes program usage patterns and maintains information about their dependencies. Figure 3 represents the prefetch file as we command "prefetch" at "run" The Prefetch file has the ".pf" extension and is placed in the " C:\Windows\Prefetch " directory. Each application has its own Prefetch file [16]. Prefetch file is very important in digital forensic as it streamline the process for software applications and programs to locate necessary data on the hard disk. Eliminating the need for programs to rely solely on the hard drive's performance during startup or hard faults, prefetch files prevent delays. Given the contemporary landscape where programs demand substantial memory and libraries, these files play a crucial role in enhancing load times.

Figure 3: Prefetch File

Tools for Prefetch file forensics:

A fundamental element within the Windows system, known as ntkrnlpa.exe, functions as a kernel process tasked with the handling of prefetch files. Its responsibilities include reading, writing, and manipulating these files according to directives from the Windows Cache Manager.

(4.4) Private Browsing

Web browsers are among the most critical pieces of software in every operating system. A web browser is required to access the internet. A forensic investigator may be required to obtain web browser history data during a forensic investigation. The article [17]suggested various ways for gathering evidence from web browsers.

Private browsing mode is designed to safeguard user data during a private browsing session by ensuring that no traces of data are left on the device being used. The article is concerned not just with history gathering, but also with the private browsing function, in which surfing data is not immediately available. The author tested private browsing mode of 03 web browser which are compatible for Windows. they are "Google Chrome"; "Mozile Firefox"; "Microsoft Edge".

Tools for Private Browsing Forensic: The author utilized two tools to retrieve lost browser data and track surfing history while private browsing. "MiniTool Power" was used to retrieve data, while "Process Monitor" was utilized to trace the history of private browsing.

Conclusion

The literature study provides a holistic view of Windows forensic and the role of Machine learning and the forensic tools for windows forensic. In summary, the importance of Windows forensic in digital forensics lies in its ubiquity, the wealth of digital artifacts it generates, and the critical role it plays in uncovering evidence related to a wide range of digital incidents. As technology evolves, so too must the field of digital forensics, with a continued emphasis on Windows forensic capabilities to address the evolving landscape of cyber threats and incidents.

5. Summary of the Review Analysis

A comprehensive review has been conducted in the paper. The Summarization is shown in the following Table 5

Table 4: Authors contribution & Applicable Tools and ML applications

1. Ref No.	Description	Applicable Tools/ML Applications	Authors Contribution
[1]	Windows Forensics Analysis	Autopsy, Access Data, Pro-discover	The authors discuss on tools for windows forensic, also mention the Work flow model for digital forensic.
[2]	Digital Forensics Investigation Procedures of Smart Grid Environment	N/A	The Author discuss the investigation procedure as per smart grid environment, where he mentioned the proper investigation procedure, which should be maintained in the field of forensic.
[3]	The role of machine learning in digital forensics	Support Vector Machine, Decision Tree, Naïve Bayes Classifications, K-nearest neighbors & artificial neural network	The author describes some Machine Learning algorithms such as: Support Vector Machine, Decision Tree, Naïve Bayes Classifications, K-nearest neighbors & artificial neural network for Link analysis, Clustering incidents and crimes, Predicting attacks and crimes and fraud detection.
[4]	Unboxing the digital forensic investigation process	N/A	The author clearly mentions the digital forensic work flow model, which is applicable for Windows forensic.
[5]	Survey on types of cyber-attacks on operating system vulnerabilities since 2018 onwards	N/A	The author provides a survey which provide us the types of cyber-attacks on OS.
[6]	A comprehensive survey on deep learning-based malware detection techniques	Ratscope, SVM, Naïve Bayes, SVM Wrapper	The author indicates malware detection procedure through ML and Deep Learning.

[7]	Dynamic Ransomware Detection for Windows Platform Using Machine Learning Classifiers	Random Forest, Naïve Bayes, J48, Decision Table and Hoeffding tree	The author discusses on ransomware detection using the Random Forest, Naïve Bayes, J48, Decision Table and Hoeffding tree.
[8]	A comprehensive survey on computer forensics: State-of-the-art, tools, techniques, challenges, and future directions	Autopsy, Redline, Belkasoft, OS-Forensic, Prodiscover, x-ways, Encase, FTK	The author provides the details of forensic tools in every sector of Digital forensic.
[9]	Forensically Important Artifacts in Windows Operating systems,	N/A	The author provides a clear definition on Artifacts, also provides us the details of windows artifacts.
[10]	A comparison of machine learning techniques for file system forensics analysis	Feed Forward Neural Network, Support Vector Machine, Random Forest, Classifications and Regression Trees	The author discusses the Feed Forward Neural Network, Support Vector Machine, Random Forest, Classifications and Regression Trees as these algorithms were chosen due to their diverse approaches in generating classifiers and their frequent use in constructing classification models.
[11]	Forensic exploration on windows File History	EFIC	Provide a clear detail of Windows File History and
[12]	An investigation into the forensic implications of the Windows 10 operating system: recoverable artefacts and significant changes from Windows 8.1	N/A	The author provides the details of event log, and its importance in Windows Operating System.
[13]	DiagAnalyzer: User behavior analysis and visualization using Windows Diagnostics logs	DiagAnalyzer:	The author developed a solution named DiagAnalyzer, which gathered information of USB, Wireless, web etc.
[14]	Automatic log parser to support forensic analysis	Nerlogparser	The author discusses the Nerlogparser, which is a Machine Learning based tools.
[15]	Process Mining of Events Log from Windows.	Event Viewer	The paper discusses on the mining process of event log, also provide a tool named “ Event Viewer” & how it works.
[16]	Digital forensic analysis on prefetch files	ntkrnlpa.exe	The paper discusses on prefetch file, their role in forensic. Also mention the detailed process to forensic it.
[17]	Forensic analysis of private browsing mechanisms: Tracing internet activities	MiniTool Power, Process Monitor	The author mentioned the private browsing and its importance regarding forensic analysis. The author provides the clear procedure of data retrieve from private browsing.

References

[1] M. Aljouhi and S. Al Hosani, “Windows Forensics Analysis,” Emirati Journal of Policing and Security Studies, vol. 1, no. 1, Nov. 2022, doi: 10.54878/EJPSS.179.

[2] H. Abdullah, Z. Ibrahim, … F. R.-… of C. and, and undefined 2021, “Digital Forensics Investigation Procedures of Smart Grid Environment,” journal.uob.edu.bhHIM Abdullah, ZA Ibrahim, FA Rahim, HS Fadzil, SAS Nizam, MZ MustaffaInternational Journal of Computing and Digital System, 2021•journal.uob.edu.bh, Accessed: Oct. 14, 2023. [Online]. Available: https://journal.uob.edu.bh/handle/123456789/4402

[3] A. Qadir, A. V. D. F. and S. (ISDFS), and undefined 2020, “The role of machine learning in digital forensics,” ieeexplore.ieee.org, doi: 10.1109/ISDFS49300.2020.9116298.

[4] G. Horsman, N. S.-S. & Justice, and undefined 2022, “Unboxing the digital forensic investigation process,” Elsevier, Accessed: Oct. 14, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1355030622000144

[5] M. Vander–Pallen, … P. A.-2022 I. W. A., and undefined 2022, "Survey on types of cyber attacks on operating system vulnerabilities since 2018 onwards," ieeexplore.ieee.orgMA Vander–Pallen, P Addai, S Isteefanos, TK Mohd2022 IEEE World AI IoT Congress (AIIoT), 2022•ieeexplore.ieee.org, Accessed: Oct. 14, 2023. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9817246/

[6] M. Gopinath and S. C. Sethuraman, "A comprehensive survey on deep learning based malware detection techniques," Comput Sci Rev, vol. 47, Feb. 2023, doi: 10.1016/j.cosrev.2022.100529.

[7] M. Jaya, M. R.-J. I. J. on Informatics, and undefined 2022, "Dynamic Ransomware Detection for Windows Platform Using Machine Learning Classifiers," joiv.orgMI Jaya, MFA RazakJOIV: International Journal on Informatics Visualization, 2022•joiv.org, Accessed: Oct. 14, 2023. [Online]. Available: http://www.joiv.org/index.php/joiv/article/view/1093

[8] A. Javed, W. Ahmed, M. Alazab, Z. Jalil, … K. K.-I., and undefined 2022, "A comprehensive survey on computer forensics: State-of-the-art, tools, techniques, challenges, and future directions," ieeexplore.ieee.org, Accessed: Oct. 23, 2023. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9678340/

[9] B. P. Kondapally, "Forensically Important Artifacts in Windows Operating systems," 2015, Accessed: Oct. 23, 2023. [Online]. Available: https://www.academia.edu/download/50204557/Forensically_Important_Artifacts_in_Windows_Operating_systems.pdf

[10] R. Mohammad, M. A.-J. of I. S. and, and undefined 2019, "A comparison of machine learning techniques for file system forensics analysis," Elsevier, Accessed: Oct. 23, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214212618307579

[11] J. Choi, J. Park, S. L.-F. S. I. D. Investigation, and undefined 2021, "Forensic exploration on windows File History," Elsevier, Accessed: Oct. 14, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2666281721000329

[12] D. Hintea, R. Bird, M. G.-S. and D. Forensics, and undefined 2017, "An investigation into the forensic implications of the Windows 10 operating system: recoverable artefacts and significant changes from Windows 8.1," inderscienceonline.com, vol. 9, no. 4, pp. 315–335, 2017, doi: 10.1504/IJESDF.2017.087394.

[13] S. Park and S. Lee, "DiagAnalyzer: User behavior analysis and visualization using Windows Diagnostics logs," Forensic Science International: Digital Investigation, vol. 43, Sep. 2022, doi: 10.1016/j.fsidi.2022.301450.

[14] H. Studiawan, F. Sohel, C. P.-16th Australian, and undefined 2018, "Automatic log parser to support forensic analysis," researchportal.murdoch.edu.au, Accessed: Oct. 19, 2023. [Online]. Available: https://researchportal.murdoch.edu.au/esploro/outputs/conferencePaper/Automatic-log-parser-to-support-forensic/991005543139307891

[15] R. Dolak, M. Janakova, J. B.- SIMPDA, and undefined 2018, "Process Mining of Events Log from Windows.," ceur-ws.org, Accessed: Oct. 18, 2023. [Online]. Available: http://ceur-ws.org/Vol-2270/short5.pdf

[16] N. Shashidhar, D. N.-I. J. of Information, and undefined 2015, "Digital forensic analysis on prefetch files," dergipark.org.trN Shashidhar, D NovakInternational Journal of Information Security Science, 2015•dergipark.org.tr, vol. 4, no. 2, Accessed: Oct. 14, 2023. [Online]. Available: https://dergipark.org.tr/en/pub/ijiss/issue/16063/167865

[17] H. Kazan, H. J. Hejase, H. Fayyad-Kazan, S. Kassem-Moussa, H. J. Hejase, and A. J. Hejase, "Forensic analysis of private browsing mechanisms: Tracing internet activities," 2021, doi: 10.29328/journal.jfsr.1001022.